 p-ISSN: 2548-9267 | e-ISSN : 2549-2365, Open Access at : *http://unramlawreview.unram.ac.id/index.php/ulrev*

Authentication of Electronic Evidence in the New Criminal Procedure Code: A Comparative Study of the United States

Shera Rendra Maharani
Universitas Negeri Surabaya
shera.22170@mhs.unesa.ac.id

Emmilia Rusdiana
Universitas Negeri Surabaya
emmiliarusdiana@unesa.ac.id.

ABSTRACT

This study examines the concept of authentication of electronic evidence within the Indonesian criminal evidentiary system under Law Number 20 of 2025 concerning the Criminal Procedure Code (Kitab Undang-Undang Hukum Acara Pidana / KUHAP) and analyses the urgency of regulating a self-authentication mechanism through hash values by conducting a comparative study with the United States Federal Rules of Evidence (FRE). The research employs a normative legal research method, drawing on statutory and comparative law. The findings demonstrate that although the new KUHAP has recognised electronic evidence as admissible, it does not specifically regulate technical authentication procedures. In contrast, Rules 902(13)–(14) of the Federal Rules of Evidence have established an efficient, standardised self-authentication mechanism based on hash values, which may be adopted and adapted within the Indonesian legal system.

Keywords: Electronic Evidence; Digital Forensics; Self-Authentication.

INTRODUCTION

The rapid development of information and communication technology has significantly transformed the Indonesian criminal justice system. The Indonesian National Police recorded 3,758 cybercrime cases in 2023, consisting of five major categories: 1,414 cases of fraud, 838 cases of defamation, 457 cases of pornography, 353 cases of illegal access, and 250 cases of gambling.[1] This condition has generated a massive amount of digital traces, ranging from digital banking transactions and location metadata to Closed-Circuit Television (CCTV) recordings, all of which have the potential to serve as evidence in judicial proceedings. However, the quality and authenticity of electronic evidence are determined through an authentication process, namely a series of procedures intended to establish that electronic evidence is genuine, has not been manipulated, and was obtained lawfully. Electronic evidence may facilitate law enforcement authorities in discovering evidence, fulfilling the minimum evidentiary threshold, and serving as the basis for the evidentiary process. Nevertheless, electronic evidence requires further verification before it may be admitted as valid evidence before the court.[2]

The Indonesian criminal justice system underwent significant reform with the enactment of Law Number 20 of 2025 concerning the Criminal Procedure Code (*Kitab Undang-*

[1]Dani Prabowo Kiki Safitri, "10 Tahun Pemerintahan Jokowi, Upaya Pemberantasan Kejahatan Siber Terus Meningkat," Kompas, 2024, https://nasional.kompas.com/read/2024/10/14/11503981/10-tahun-pemerintahan-jokowi-upaya-pemberantasan-kejahatan-siber-terus?page=all.

[2]Nurlaila Isima, "KEDUDUKAN ALAT BUKTI ELEKTRONIK DALAM PEMBUKTIAN PERKARA PIDANA," *Gorontalo Law Review* 5, no. 1 (2022): 179–89, https://doi.org/https://doi.org/10.32662/golrev.v5i1.1999.

DOI: https://doi.org/10.29303/ulrev.v101.499

Undang Hukum Acara Pidana / KUHAP), which came into force on 2 January 2026.[3] One of the most substantial changes concerns the evidentiary system. Under the former Criminal Procedure Code of 1981, only five categories of admissible evidence were recognised. Article 184 paragraph (1) stipulated that: "Valid evidence shall consist of: (a) witness testimony; (b) expert testimony; (c) documents; (d) indications; and (e) the statement of the accused."[4] In contrast, the new KUHAP recognizes eight categories of evidence as provided under Article 235 paragraph (1): "Evidence shall consist of: (a) witness testimony; (b) expert testimony; (c) documents; (d) the statement of the accused; (e) physical evidence; (f) electronic evidence; (g) judicial observation; and (h) any matter that may be used for evidentiary purposes during court proceedings insofar as it is obtained lawfully."[5] This amendment reflects a shift from a closed evidentiary system to an open evidentiary system. The new KUHAP requires that every item of evidence must be authenticated and obtained lawfully. However, the admissibility and validity of electronic evidence presented at trial ultimately remain subject to judicial discretion. This condition puts electronic evidence in a vulnerable position, particularly given that it may be altered or fabricated using artificial intelligence technologies. In the absence of clear digital forensic standards and authentication procedures, disparities in law enforcement practice may arise.[6] The use of electronic evidence as an extension of admissible evidence must therefore observe several principles: (1) data integrity, requiring law enforcement officials to maintain the integrity and authenticity of electronic evidence; (2) management by digital forensic experts; and (3) compliance with prevailing statutory regulations.[7] Furthermore, evidence presented before the court must satisfy the criteria of admissible evidence, namely: (1) admissibility, meaning that the evidence is legally permissible under statutory law; (2) reliability, meaning that the evidence can be trusted as authentic; (3) necessity, meaning that the evidence is necessary to establish a fact; and (4) relevance, meaning that the evidence bears a connection to the facts at issue.[8] One notable example is the criminal case involving the YouTuber Resbob, in which defence counsel argued that no examination of the electronic evidence had been conducted, including metadata analysis and digital forensic validation. The defence requested an examination of the metadata and hash values of the documents submitted as evidence and sought the involvement of independent experts to assess the admissibility of the electronic evidence.[9] This case demonstrates that Indonesian law requires clear technical guidelines and standards for assessing the authenticity and validity of electronic evidence. Such technical standards would strengthen the consistency of judicial decisions throughout Indonesia.

On the other hand, the United States has comprehensively regulated authentication through the Federal Rules of Evidence (FRE). The FRE adopts the concept of self-authentication for electronic evidence through hash-value–based certification, which serves as an efficient mechanism in criminal proceedings. This is specifically regulated under Rule 902 concerning "Evidence That is Self-Authenticating," particularly Rule 902(13) regarding "Certified Records Generated by an Electronic Process or System" and Rule 902(14) regarding "Certified

[3]Sekertariat Negara, "KUHP Dan KUHAP Baru Resmi Berlaku, Penegakan Hukum Di Indonesia Masuki Era Baru," 2026, https://www.setneg.go.id/baca/index/kuhp_dan_kuhap_baru_resmi_berlaku_penegakan_hukum_di_indonesia_masuki_era_baru.

[4]"Undang-Undang Nomor 8 Tahun 1981 Tentang Hukum Acara Pidana" (1981). Pasal 184

[5]"Undang-Undang Nomor 20 Tahun 2025 Tentang Kitab Hukum Acara Pidana" (2025). Pasal 235

[6]Lasta Elfrida Sinaga, "KUHAP 2025 Mengakui Bukti Elektronik: Bagaimana Autentikasinya?," Mangatur Nainggolan Law Firm, 2026, https://mnllaw.co.id/kuhap-2025-mengakui-bukti-elektronik-bagaimana-autentikasinya/.

[7]Dewantoro, "AUTENTIKASI ALAT BUKTI ELEKTRONIK DALAM MEMPERLANCAR PEMBUKTIAN DI PERSIDANGAN PADA ERA DISRUPSI," *Jurnal Hukum Progresif* 12, no. 2 (2024): 135–51, https://doi.org/https://doi.org/10.14710/jhp.12.2.135-151.

[8]Munir Fuady, *Teori Hukum Pembuktian Pidana Dan Perdata*, Cet. 2 (Bandung: Citra Aditya Bakti, 2012).

[9]Erik A Kurnia, "Eksepsi Resbob, Lokasi Perkara Dipersoalkan, Bukti Elektronik Diminta Diuji Ulang," RadarSumedang.id, 2026, https://www.radarsumedang.id/bandung/2026/03/05/eksepsi-resbob-lokasi-perkara-dipersoalkan-bukti-elektronik-diminta-diuji-ulang/.

Data Copied from an Electronic Device, Storage Medium, or File." These provisions permit electronic evidence to be admitted in court through written certification by a qualified forensic expert without requiring the expert's direct appearance at trial. Consequently, the mechanism enhances judicial efficiency while ensuring the integrity of electronic evidence through certifications issued by competent forensic experts. The Federal Rules of Evidence in the United States are further supported and reinforced by technical standards developed by the National Institute of Standards and Technology (NIST). NIST guidelines are frequently used to ensure security controls and data integrity within federal institutions and have gained international recognition. While Rules 902(13)–(14) explicitly regulate the concept of hash–value–based self-authentication, the underlying technical standards of the FRE possess international characteristics through their harmonisation with ISO/IEC standards. Therefore, the author selects the Federal Rules of Evidence as the comparative legal model in this study.

Relevant previous studies include the research conducted by Sacvio Fath Senajaya et al. (2026), which emphasised the need to reform digital forensic regulations in the evidentiary process for corruption cases within the Office of the Attorney General of the Republic of Indonesia.[10] The study also recommended adopting the Federal Rules of Evidence within the Indonesian criminal evidentiary system, though it did not elaborate further on the model. In addition, research conducted by Vanessa and Henry Firmansyah (2025) identified inconsistencies in the treatment of electronic evidence across two court decisions. In the first decision, electronic evidence was admitted without forensic examination, whereas in the second decision, the evidence was admitted only after undergoing digital forensic analysis.[11] This study demonstrated inconsistencies in the evidentiary assessment of electronic evidence but did not provide an international comparative model. Furthermore, research by Yanto Irianto (2025), conducted at the Cirebon District Court, revealed challenges in establishing the authenticity and technical verification of electronic evidence.[12] The study focused primarily on weaknesses in technical verification and emphasised the need for stronger procedural guidelines in Indonesia, but it did not propose self-authentication as a solution. Collectively, these studies indicate that Indonesian law requires technical guidelines for the standardisation of electronic evidence authentication. Accordingly, this study proposes adopting the self-authentication concept developed in the United States by examining the new Indonesian Criminal Procedure Code and comparing it with the United States Federal Rules of Evidence.

Based on the foregoing background, this study addresses the following research questions: (1) What is meant by the authentication of electronic evidence under the 2025 Indonesian Criminal Procedure Code and the United States Federal Rules of Evidence? (2) What is the urgency of regulating the concept of self-authentication through hash values within Indonesian criminal procedural law?

METHOD

This study employs a normative legal research method, which focuses on the examination of primary and secondary legal materials. The research applies a statutory approach by analysing the 2025 Indonesian Criminal Procedure Code (*Kitab Undang-Undang Hukum Acara Pidana*

[10]Slamet Tri Wahyudi Sacvio Fath Senajaya, Handar Subhandi Bakhtiar, "Reformulasi Peraturan Digital Forensic Di Dalam Proses Pembuktian Perkara Tindak Pidana Korupsi Di Kejaksaan Agung Republik Indonesia," *Jurnal Kajian Hukum Dan Kebijakan Publik* 3, no. 2 (2026): 473–86, https://doi.org/https://doi.org/10.62379/av9bjg92.

[11]Vanessa Vanessa and Hery Firmansyah, "Analysis of the Validity of Electronic Evidence in Criminal Trial Proceedings and the Implementation of Its Admissibility (Judgment Study)," *Indonesian Jurnal Law and Economics Review* 20, no. 4 (2025), https://doi.org/https://doi.org/10.21070/ijler.v20i4.1395.

[12]Yanto Irianto, "Judicial Adaptation to Digital Evidence in the Era of Cyber Governance," *Formosa Journal of Science and Technology (FJST)* 4, no. 9 (2025): 3015–30, https://doi.org/https://doi.org/10.55927/fjst.v4i9.248.

/ KUHAP) and the United States Federal Rules of Evidence. In addition, a comparative approach is utilised to systematically compare the electronic evidence authentication systems in Indonesia and the United States. The legal materials consist of primary statutory regulations, while secondary materials include legal literature, scientific journals, and scholarly books.

ANALYSIS AND DISCUSSION

Authentication of Electronic Evidence in the New Criminal Procedure Code 2025 and the United States Federal Rules of Evidence

Authentication of Electronic Evidence in the New Criminal Procedure Code 2025

In the evidentiary process involving electronic evidence, authentication is considerably more complex than the authentication of physical evidence. Physical evidence may generally be authenticated through visual examination, simple laboratory testing, or testimony from individuals familiar with the object. In contrast, electronic evidence in the form of digital data cannot be verified solely through visual inspection to ensure its integrity and authenticity, since modifications to digital data do not leave visible physical traces. An electronically manipulated document may appear visually genuine; therefore, specialised methods are required to verify its integrity and authenticity.[13] The recognition of electronic evidence under the 2025 Criminal Procedure Code (*Kitab Undang-Undang Hukum Acara Pidana* / KUHAP) has effectively ended the longstanding debate concerning the legal status of electronic evidence within the Indonesian criminal justice system. The explanation regarding electronic evidence is provided under Article 242 of the new KUHAP, which stipulates that: "Electronic evidence as referred to in Article 235 paragraph (1) letter f includes all forms of Electronic Information, Electronic Documents, and/or electronic systems related to criminal offences." Article 242 expands the scope of electronic evidence, reflecting the continuous evolution of electronic systems alongside advancements in information technology. Electronic evidence may include WhatsApp or Telegram messages, digital metadata, body camera recordings, drone evidence, digital footprints, and scientific evidence such as DNA, ballistics, and toxicology reports.[14] The provisions under Article 56 letter (e) of the KUHAP further provide that: "Technical investigative assistance as referred to in Article 55 shall include: (a) forensic laboratories, used when investigators require examination and testing of evidence requiring special handling and/or treatment; (b) identification, used when investigators require certainty regarding the identity of suspects, witnesses, or victims of criminal offenses and as evidentiary tools; (c) forensic medicine, used when investigators require examination of suspects, witnesses, or victims requiring special physical treatment; (d) forensic psychology, used when investigators require examination of suspects, witnesses, or victims requiring special psychological treatment; (e) digital forensics, used when investigators require examination and testing of digital evidence requiring special handling or treatment; and (f) other technical assistance as required." Such assistance is utilized where investigators require examination and testing of digital evidence that necessitates special handling. The use of the term "require" emphasizes the non-mandatory nature of digital forensic assistance, rendering it discretionary when deemed necessary by investigators rather than constituting an obligatory requirement in every case involving electronic evidence.[15]

[13]Casey Eoghan, *Digital Evidence and Computer Crime* (United States of America: Academic Press, 2011).
[14]Muladi & Barda Nawawi Arief, *Teori-Teori Dan Kebijakan Pidana*, 4th ed. (Bandung: Alumni, 2010).
[15]Sinaga, "KUHAP 2025 Mengakui Bukti Elektronik: Bagaimana Autentikasinya?"

Nevertheless, the new KUHAP does not regulate specific procedures for the authentication of electronic evidence nor establish digital forensic standards to ensure its authenticity and integrity. Consequently, evidentiary proceedings in court may encounter significant obstacles, particularly in cybercrime cases in Indonesia. Under the new KUHAP, judges possess the authority to determine the authenticity of electronic evidence, as stipulated in Article 235 paragraph (4): "Judges shall have the authority to assess the authentication and the legality of the acquisition of evidence presented." Furthermore, evidence deemed inauthentic may not be used during trial proceedings pursuant to Article 235 paragraph (5), which provides that: "Evidence declared by the judge to be inauthentic and/or unlawfully obtained may not be used as evidence in court proceedings and shall possess no evidentiary value.*"*[16] Judicial conviction is therefore not established solely by the quantity of evidence presented, but also by the quality and validity of the electronic evidence itself. Accordingly, the regulation of digital forensic standards constitutes an essential component of the principle of due process of law.[17] The 2025 KUHAP resolves the previous ambiguity by expressly recognising electronic evidence as an independent category of evidence under Article 235 paragraph (1) letter (f). This recognition eliminates the need to force electronic evidence into the traditional categories of documentary or circumstantial evidence, instead establishing it as a distinct evidentiary category with its own specific requirements and procedures.

The authentication requirement under Article 235 paragraph (3), which stipulates that: "Evidence as referred to in paragraph (1) must be capable of authentication and obtained lawfully."[18], constitutes a substantive legal obligation that must be fulfilled before evidence may acquire evidentiary value. The judicial gatekeeping authority granted under Article 235 paragraph (4) positions judges as active gatekeepers responsible for assessing the admissibility and reliability of evidence. This provision shifts the paradigm from judges acting merely as passive evaluators to judges functioning as active filters in determining evidentiary admissibility. Moreover, the exclusionary rule codified under Article 235 paragraph (5) operates as a normative sanction ensuring compliance with authentication standards and the legality of evidence acquisition. However, the new KUHAP still does not regulate specific procedures for authenticating electronic evidence, including data imaging, digital sealing using hash values, preservation procedures to maintain data integrity, and chain of custody documentation. Understanding the technical characteristics of digital evidence is, therefore, essential for establishing proper and effective authentication procedures. Several distinctive characteristics of digital evidence include:

1. Volatility, whereby digital data may easily change or be deleted, even though actions that appear harmless, such as turning on a computer or accessing a network.
2. Perfect duplicability, meaning that digital copies are identical bit-by-bit to the original data, unlike physical documents whose copies may be distinguished from the originals.
3. Metadata, whereby every digital file contains metadata recording information regarding creation time, modification, access, and other technical attributes.
4. Dependence upon specialised devices, as certain digital evidence cannot be accessed without appropriate hardware and software; and.
5. Cross-jurisdictional characteristics, since digital data may be stored on servers located in foreign jurisdictions, thereby complicating access and collection procedures.

These characteristics require a specialised approach in the management and authentication of electronic evidence to ensure evidentiary validity. Electronic evidence must satisfy four

[16]Undang-Undang Nomor 20 Tahun 2025 tentang Kitab Hukum Acara Pidana. Pasal 235 ayat 5
[17]Sacvio Fath Senajaya, Handar Subhandi Bakhtiar, "Reformulasi Peraturan Digital Forensic Di Dalam Proses Pembuktian Perkara Tindak Pidana Korupsi Di Kejaksaan Agung Republik Indonesia."
[18]Undang-Undang Nomor 20 Tahun 2025 tentang Kitab Hukum Acara Pidana. Pasal 235 ayat 3

interrelated requirements: authenticity, integrity, accessibility, and legality of acquisition. Among these requirements, integrity verification is the most technical and fundamental, because without assured integrity, the authenticity and evidentiary value of electronic evidence become unreliable.[19] Without digital forensic examination, the evidentiary value of electronic evidence may be questioned regarding its authenticity and completeness, particularly when metadata or encryption data become unclear or suddenly disappear. Evidence obtained without lawful forensic procedures also carries the risk of manipulation or modification by unauthorised parties. To overcome these challenges, digital forensic examination should be conducted as an initial authentication process during judicial proceedings. Authentication is a formal procedural requirement; however, in practice, it is frequently neglected.[20] Where substantive requirements are fulfilled, electronic evidence is generally considered admissible. International forensic literature and guidelines such as ISO/IEC 27037 emphasise that the identification, collection, preservation, and verification of digital evidence must be conducted from the outset through properly documented procedures. Verification of digital evidence integrity principally relies upon hash values as the primary instrument, as standardised under ISO/IEC 27037:2012.[21] Research on Solid State Drive (SSD) forensics conducted by Sunardi et al. further confirms that digital evidence validation using hash algorithms produces identical hash values when evidence has not been altered. Consequently, the integrity verification results demonstrate that the digital evidence remains identical to the original source.[22] The assessment of electronic evidence, therefore, requires a comprehensive understanding that extends beyond formal procedural considerations to encompass substantive technical aspects. Within the administrative sphere, Supreme Court Regulation (*Peraturan Mahkamah Agung* / PERMA) Number 7 of 2022 concerning Electronic Case Administration and Court Proceedings provides a technical framework for electronic court proceedings (*e-court* and *e-litigation*). This regulation permits the electronic submission of claims, responses, replies, rejoinders, and evidence. However, the PERMA primarily focuses on administrative procedures and does not comprehensively regulate authentication processes for the authenticity of digital evidence, such as metadata authentication, hash value validation, or chain-of-custody procedures.[23]

The evidentiary process constitutes the core of the judicial system and serves the essential function of upholding justice. This process involves not only the collection and presentation of evidence, but also the resolution of challenges relating to witness credibility and the validity of electronic evidence. In the digital era, the validity of electronic evidence has become increasingly significant because evidence constitutes a determining factor in achieving justice for litigating parties.[24] Law without legal certainty loses its meaning because it can no longer function as a guideline for society. Legal certainty, therefore, constitutes one of the fundamental

[19]Desti Mualfah and Rizdqi Akbar Ramadhan, "Analisis Forensik Metadata Kamera CCTV Sebagai Alat Bukti Digital," *Digital Zone: Jurnal Teknologi Informasi Dan Komunikasi* 11, no. 2 (2020): 257–67, https://doi.org/https://doi.org/10.31849/digitalzone.v11i2.5174.

[20]Vanessa and Firmansyah, "Analysis of the Validity of Electronic Evidence in Criminal Trial Proceedings and the Implementation of Its Admissibility (Judgment Study)."

[21]Faizul Idris et al., "ANALISIS KEBERHASILAN DAN KEGAGALAN BUKTI FORENSIK DIGITAL DALAM SISTEM PERADILAN INDONESIA 'Study Kasus Putusan Nomor 130/Pid.Sus/2023/PN Ckr & Putusan Nomor 82/Pdt.G/2024/PA.Prob,'" *Journal of Golden Generation Legal Science* 2 (2026): 71–89, https://doi.org/https://doi.org/10.65244/jggls.v2i1.70.

[22]Imam Mahfudi Nasrulloh, Sunardi Sunardi, and Imam Riadi, "ANALISIS FORENSIK SOLID STATE DRIVE (SSD) MENGGUNAKAN FRAMEWORK GRR RAPID RESPONSE FORENSIC ANALYSIS OF SOLID STATE DRIVES (SSD) USING THE GRR RAPID RESPONSE FRAMEWORK," *Jurnal Teknologi Informasi Dan Ilmu Komputer* 6, no. 5 (2019): 509–18, https://doi.org/10.25126/jtiik.201961516.

[23]Irianto, "Judicial Adaptation to Digital Evidence in the Era of Cyber Governance."

[24]Melki T. Tunggati, "Legal Validity of the Use of Graphonomy as an Evidentiary Instrument in Business Disputes in the Digital Age," *UNRAM LAW REVIEW* 9, no. 1 (2025), https://doi.org/https://doi.org/10.29303/ulrev.v9i1.404.

objectives of law in realising justice.[25] With clear guidelines governing the authentication of electronic evidence, disparities in judicial assessment of electronic evidence may be reduced. This would strengthen consistency in law enforcement and the administration of justice in Indonesia. Through harmonised understanding and strengthened institutional capacity, the evidentiary framework under the new KUHAP may enhance public trust in judicial institutions. Inter-agency cooperation in handling criminal cases in Indonesia has indeed been established through Memoranda of Understanding; however, such cooperation has yet to provide adequate authority for digital forensic laboratories. Ultimately, the success of criminal prosecution depends not only on the existence of evidence, but also on the manner in which such evidence is handled, in compliance with the principle of legality and standardised procedures.[26]

Authentication of Electronic Evidence under the Federal Rules of Evidence

The United States has developed advanced digital forensic standards through regulations and guidelines issued by the National Institute of Standards and Technology (NIST). In addition, the United States provides a legal foundation for the authentication of electronic evidence through the Federal Rules of Evidence (FRE), particularly Rules 901 and 902. This demonstrates that the effectiveness of digital forensic practices depends upon synchronisation between technical guidelines and evidentiary rules. Rule 901(a) provides: "In General. To satisfy the requirement of authenticating or identifying an item of evidence, the proponent must produce evidence sufficient to support a finding that the item is what the proponent claims it is."[27] Rule 901 reflects the concept of *extrinsic evidence authentication*, whereby the party presenting the evidence must produce external evidence, such as expert testimony, to establish the authenticity of electronic evidence. However, on 1 December 2017, the United States amended the Federal Rules of Evidence by introducing Rule 902(13) concerning "Certified Records Generated by an Electronic Process or System" and Rule 902(14) concerning "Certified Data Copied from an Electronic Device, Storage Medium, or File," both of which specifically regulate self-authentication for electronic evidence. Rule 902 generally governs *self-authenticating evidence*. Prior to the 2017 amendment, the Rule primarily applied to public documents, official publications, and certified business records. Nevertheless, rapid technological advancement transformed electronic evidence into a central component of modern litigation. Consequently, the Judicial Conference Advisory Committee on Evidence Rules formulated a comprehensive mechanism for self-authentication of electronic evidence.[28] Rule 902 governs self-authentication to address procedural efficiency in modern litigation, allowing certain categories of evidence to be authenticated without the need for additional extrinsic evidence because their origin and nature already provide sufficient guarantees of authenticity. Before the 2017 amendment, authentication of electronic evidence under the FRE largely relied on Rule 901(b)(9), a mechanism that required expert witnesses at trial, thereby consuming substantial time and costs. Rule 902(13) concerns "Certified Records Generated by an Electronic Process or System," namely, records generated by an electronic process or system that produces accurate results, as demonstrated through certification by a qualified person. Meanwhile, Rule 902(14) governs "Certified Data Copied from an Electronic Device, Storage Medium, or File," namely, data copied from electronic devices, storage media, or files that are authenticated through a digital identification process, as demonstrated through

[25]Mutiaratu Astari Rafli, "Legality Of Authentic Deed With Cyber Notary Basis According To Legal Assurance Principles," *UNRAM LAW REVIEW* 6, no. 1 (2022), https://doi.org/https://doi.org/10.29303/ulrev.v6i1.225.

[26]Sacvio Fath Senajaya, Handar Subhandi Bakhtiar, "Reformulasi Peraturan Digital Forensic Di Dalam Proses Pembuktian Perkara Tindak Pidana Korupsi Di Kejaksaan Agung Republik Indonesia."

[27]National Court Rules Committee, "Federal Rules of Evidence" (2024), https://www.rulesofevidence.org/.

[28]Daniel J. Capra Hon. Paul W. Grimm, Gregory P. Joseph, *Best Practices for Authenticating Digital Evidence.Pdf* (St. Paul,MN55101: West Academic Publishing, 2016).

certification by a qualified person who satisfies the requirements under Rule 902(11) or Rule 902(12).[29] Self-authentication under Rules 902(13)–(14) constitutes a procedural efficiency, as parties presenting electronic evidence no longer need to summon digital forensic experts to testify directly before the court. Instead, it is sufficient to submit a written certification from a qualified person explaining that the evidence has undergone authentication procedures in accordance with digital forensic standards, including hash value verification. Nevertheless, opposing parties retain the right to challenge the authentication and request the presentation of expert testimony where necessary.[30] A "qualified person" generally refers to a digital forensic examiner possessing professional certifications such as CFCE (*Certified Forensic Computer Examiner*), EnCE (*EnCase Certified Examiner*), or GCFE (*GIAC Certified Forensic Examiner*), or alternatively, an internal information technology specialist or e-discovery vendor possessing adequate technical expertise. The certification must describe the data acquisition process, the tools utilised, and the results of the hash value verification. *Rule 902(13) specifically provides:* ***Certified Records Generated by an Electronic Process or System.*** *A record generated by an electronic process or system that produces an accurate result, as shown by a certification of a qualified person that complies with the certification requirements of Rule 902(11) or (12). The proponent must also meet the notice requirements of Rule 902(11)"*[31] Certification under Rule 902 serves solely to establish that the evidence presented is authentic. In Indonesia, courts still occasionally admit electronic evidence without adequately verifying its authenticity or integrity. Accordingly, this concept may serve as a model to ensure that judges admit electronic evidence only after its authenticity and integrity have been properly established.

Rule 902(14) provides: "**Certified Data Copied from an Electronic Device, Storage Medium, or File**. *Data copied from an electronic device, storage medium or file, if authenticatied by a process of digital identifcation, as shown by a certification of a qualified person that complies with the certification requirements of Rule (902(11) or (12). The proponent also must meet the notice requirements of Rule 902 (11)"* he scope of Rule 902(14) includes copies of data derived from hardware devices, such as hard drives or flash drives, as well as copies of electronic files. The fundamental element underlying Rules 902(13) and 902(14) is the use of *hash values*. Electronic evidence intended for use in court proceedings must undergo certification to ensure its authenticity. This mechanism prevents parties from presenting falsified evidence while simultaneously simplifying judicial proceedings. The essence of Rule 902(14) lies in the use of hash values, as reflected in the statement that"*Today, data copied from electronic devices, storage media, and electronic files are ordinarily authenticated by "hash value Technically, hash values commonly used in digital forensics include MD5 (128-bit output), SHA-1 (160-bit output), and SHA-256 (256-bit output). A hash value is a unique numerical value generated by a cryptographic hash function when applied to specific data. Cryptographic hashing serves important functions within digital forensics and possesses two principal mathematical characteristics. First, it is deterministic, meaning that identical input will always produce identical output. Second, it is collision-resistant, meaning that it is computationally infeasible to produce two different inputs generating the same hash value. Consequently, a hash value functions as a unique digital fingerprint; even the slightest alteration to the data, including a one-bit change, will generate an entirely different hash value.*[32] Rule 902(14) implicitly recognises hash values as a valid method within digital forensic practice. Such recognition is consistent with standards developed by the National Institute of Standards and Technology

[29]Committee, Federal Rules of Evidence.
[30]Daniel Capra, *Authenticating Digital Evidence* (Baylor Law Rev, 2017).
[31]Committee, Federal Rules of Evidence.
[32]Quynh Dang, "Recommendation for Applications Using Approved Hash Algorithms" (National, 2012), https://doi.org/https://doi.org/10.6028/NIST.SP.800-107r1.

(NIST). One of the simplest methods for demonstrating that electronically stored information (ESI) is identical to the original source is to apply hash algorithms.

An illustration of the application of Rule 902(14) to authenticate copied data is as follows. Forensic technician Smith created a forensic copy of Dain's Samsung Galaxy smartphone in the field in San Diego. Smith verified that the forensic copy was identical to the original text message logs contained within the phone using industry-standard methodologies, such as hash value verification. Smith subsequently transmitted the copy to forensic technician Jones, who conducted the forensic examination in his Atlanta laboratory. Jones relied exclusively on the forensic copy throughout the examination process to avoid inadvertently altering the original data on the phone. During the examination, Jones discovered relevant text messages. The prosecution intended to introduce the forensic copy as part of the evidentiary foundation for Jones's testimony regarding the text messages identified during the examination. Without Rule 902(14), the prosecution would have been required to present two witnesses. First, forensic technician Smith would need to testify about the creation of the forensic copy and the methodology used to verify that the copy accurately replicated the data on Dain's phone. Second, the prosecution would need to call forensic technician Jones to testify about the forensic examination. However, under Rule 902(14), the prosecution may instead obtain a written certification from Smith describing the process used to copy and verify the phone data accurately. Prior to trial, the prosecution would provide both the certification and reasonable notice to the opposing party, namely the defendant Ian, regarding its intention to introduce the exhibit at trial. If Ian's counsel failed to timely challenge the reliability of the process used to generate the Samsung Galaxy text message logs, the prosecution would only be required to summon forensic technician Jones. Depending on the litigation strategy, the prosecution might also seek to authenticate the text message logs under Rule 902(13).[33]

Urgency of Regulating The Concept of Self-Authentication Through Hash Values in Criminal Procedure Law in Indonesia

In digital forensics, the use of hash values is based upon the following principle: when an electronic device is seized, forensic investigators employ specialised software known as a *write blocker* to create a bit-by-bit copy (*forensic image*) of the device without altering the original data. Subsequently, the SHA-256 algorithm is applied to the forensic image to generate a hash value. The resulting hash value is recorded as a "digital fingerprint" within the chain of custody documentation. Each time the forensic image is accessed for analysis, the hash value is recalculated. If the recalculated value is identical to the hash value recorded at the time of seizure, it is mathematically proven that the data has not undergone any alteration since its acquisition.[34] To ensure document integrity and authentication, particularly within legal institutions, SHA-256 is widely used because its change-detection capabilities demonstrate high consistency and reliability.[35] Research on CCTV metadata forensics, integrating the provisions of SNI ISO 27037:2014, further establishes that the chain of custody for digital evidence must chronologically document all interactions with the evidence, including the identities of individuals accessing it, the times and locations of access, the purposes of access,

[33]John M Haried, "HOW TWO NEW RULES FOR SELF-AUTHENTICATION WILL SAVE YOU TIME AND MONEY," *Bolch Judicial Institute at Duke Law* 100, no. 4 (2021): 34–42.

[34]Devi Maulitasari and Rossi Passarella, *Teori Dan Sejarah Citra Forensik*, Pertama (Palembang: Unsri Press, 2020), https://repository.unsri.ac.id/92388/1/Teori dan Sejarah Citra Forensik.pdf.

[35]Habiburrahman Habiburrahman, "MD5 Di Era Post-Kriptografi : Studi Efektivitas Untuk Perlindungan Arsip Elektronik Pendahuluan," *Jurnal Ilmu Informasi Perpustakaan Dan Kearsipan* 14, no. 01 (2025): 9–18, https://doi.org/https://doi.org/10.24036/jiipk.v14i1.133546.

and the integrity verification methods utilised. This standard may therefore serve as a reference point for the development of national regulations.[36]

The new KUHAP creates legal uncertainty for all parties involved in criminal proceedings. Investigators lack clear guidelines for handling digital evidence, and public prosecutors similarly lack standardised parameters for presenting electronic evidence at trial. Judges are not provided with objective criteria for assessing whether authentication procedures have been properly conducted, and defendants remain uncertain about the standards judges apply. Such uncertainty is inconsistent with the principle of *due process of law*, which requires clarity and predictability in legal procedures. To ensure uniform application throughout Indonesia, technical guidelines are required to determine the admissibility of electronic evidence in judicial proceedings. Such technical guidelines should contain clear standards regarding evidentiary completeness and substantive requirements. Furthermore, these guidelines should regulate methods for verifying data content, including metadata examination, time and location verification, identification of relevant actors, and device validation. These regulations are intended to guarantee the authenticity, integrity, and availability of electronic information. Accordingly, a digital forensic examination is necessary to ensure that these requirements are met. This mechanism would provide legal certainty for law enforcement authorities while simultaneously protecting the rights of suspects, defendants, and victims. From a cybersecurity governance perspective, the weak integration between legal norms and practical implementation underscores that Indonesia's digital justice system remains fragmented. Cybersecurity requires synergy between legal regulations, technological infrastructure, and human resource capacity. Without a proper balance among these three elements, judicial proceedings become vulnerable not only to inconsistency but also to challenges concerning the legitimacy of judicial decisions. Consequently, strategic measures are required, including technical standards for digital evidence authentication, training for law enforcement personnel, and the establishment of specialised digital forensic units within local courts to strengthen the credibility of digital evidence before the law.[37] The concept of self-authentication has proven capable of significantly reducing litigation burdens. In the absence of self-authentication mechanisms, every case involving electronic evidence requires the presentation of digital forensic experts to testify regarding authentication procedures, resulting in increased costs and prolonged proceedings. Given the increasing number of cybercrime cases in Indonesia, adopting self-authentication concepts would substantially enhance the efficiency of the criminal justice system. Standardisation of electronic evidence authentication procedures would also strengthen Indonesia's capacity to handle cases involving electronic evidence. Authentication standards harmonised with international standards, such as the Federal Rules of Evidence, would greatly facilitate this process. Documented digital chain-of-custody procedures may create an auditable record capable of accounting for every action performed on electronic evidence. This serves not only as a preventive mechanism against evidence manipulation but also as an effective supervisory mechanism over investigative conduct. Clear, measurable authentication standards would also provide stronger protections for defendants. Through objective standards, defendants and defence counsel would more easily assess whether investigative procedures complied with established standards. Consequently, defendants would be better able to exercise their right to challenge inauthentic or unlawfully obtained evidence. This is consistent with the principle of the *exclusionary rule* codified under Article 235 paragraph (5). The concept of self-authentication under FRE Rule 902 comprises two distinct layers. The first layer concerns

[36]Mualfah and Ramadhan, "Analisis Forensik Metadata Kamera CCTV Sebagai Alat Bukti Digital."
[37]Irianto, "Judicial Adaptation to Digital Evidence in the Era of Cyber Governance."

the technical principles of digital proof serving as the foundation for self-authentication, such as hash values, chain of custody, and data integrity. These principles are technically universal. The second layer concerns procedural evidentiary mechanisms governing how such technical principles are operationalised within judicial proceedings, including who bears the burden of proof, how and when authentication is conducted, and to whom evidentiary burdens shift. This second layer is influenced by each country's legal system. These questions are answered very differently within common law and civil law systems. Nevertheless, the principles of digital forensics are universal, including data integrity through cryptographic hashing, the chain of custody as a universal forensic principle, and international standardisation reflected in ISO/IEC 27037 as a point of convergence. ISO standards are recognised across jurisdictions with differing legal traditions, including both common law and civil law systems. In Germany, for instance, authentication frequently relies on cryptographic hash verification to ensure that electronic evidence remains intact and unaltered.[38]

There are, however, certain limitations that must be avoided. Self-authentication under FRE Rule 902 operates through a mechanism of *rebuttable presumption*, namely a presumption of authenticity that may be challenged by the opposing party. In civil law systems, judges generally conduct a free and comprehensive evaluation of all evidence without waiting for objections from opposing parties. Furthermore, the concept of a "qualified person" may create institutional distortions in jurisdictions where certified e-discovery vendors do not exist or where forensic experts are regulated through different mechanisms. The principle commonly recognised in civil law traditions as *vrij bewijsstelsel*, *liberté de la preuve*, or *freie Beweiswürdigung* fundamentally differs from the logic underlying self-authentication. Under self-authentication, electronic evidence is presumed authentic unless rebutted, whereas under systems applying free evaluation of evidence, judges independently assess all evidence without being bound by formal presumptions. These two principles cannot operate simultaneously without substantial modification. In continental criminal law systems, guarantees of fair trial rights and the accused's right to challenge evidence are protected through constitutional mechanisms different from the American *Confrontation Clause*. Consequently, the transplantation of self-authentication mechanisms without regard for the constitutional framework of evidentiary rights may generate normative conflicts.

In light of these limitations, adaptations rather than direct legal transplants should be implemented. From a universal technical perspective, adaptation may include establishing authentication standards by mandating the use of minimum SHA-256 hash algorithms for the integrity verification of electronic evidence during criminal investigations, in accordance with NIST recommendations (2015) and international standards. Meanwhile, the use of MD5 and SHA-1 should be prohibited for legal forensic purposes due to their cryptographic vulnerabilities. Standardisation of digital chain of custody procedures should additionally require documentation of at least: The identity of officers conducting the seizure; The time and location of seizure; A description of the seized devices; The hash value is calculated at the time of seizure; Every access made to the digital evidence; Recalculated hash values for each access; and The storage location and storage conditions of the digital evidence, in accordance with SNI ISO 27037:2014. Furthermore, minimum qualification standards for digital forensic experts and notification requirements to opposing parties prior to trial concerning electronic evidence should also be regulated. Several concepts should be transformed rather than directly transplanted into the Indonesian legal system. The concept of *rebuttable presumption*

[38]Jens Ferner, "Digital Evidence in Germany: Legal Foundations, Collection, and Admissibility in Court," Ferner Alsdorf, 2025, https://www.ferner-alsdorf.com/digital-evidence-in-germany-legal-foundations-collection-and-admissibility-in-court/#:~:text=Post-mortem imaging (creating bit,the defense effectively raises doubt.

of authenticity should be reformulated into a presumption that may be rejected *ex officio* by the judge. Notice requirements to opposing parties should be modified so that they are submitted through the judge as procedural coordinator, rather than directly between litigating parties. Certification by a "qualified person" should be adapted to a court-appointed expert system comparable to the *gerichtlicher Sachverständiger* or *expert judiciaire*. Likewise, self-authentication without live testimony should be rephrased as a technical presumption that shifts the burden of verification to the judge. Finally, judges must be expressly recognised as evidentiary gatekeepers by providing objective parameters for assessing the authentication of electronic evidence before deciding whether to admit or exclude it. Such parameters may include: Has the hash value been properly verified? Has the chain of custody been comprehensively documented? Does the expert conducting the authentication possess recognised certification? These objective standards would provide legal certainty while simultaneously strengthening the judicial gatekeeping function.

CONCLUSION

Based on the comparative and normative analysis conducted in this study, two principal conclusions may be drawn. First, the authentication of electronic evidence under the 2025 Criminal Procedure Code (*Kitab Undang-Undang Hukum Acara Pidana* / KUHAP) has been formally recognised through Article 235 paragraph (3), which requires that electronic evidence must be authenticated and obtained lawfully. Judges are granted authority to assess authentication under Article 235, paragraph (4), while the *exclusionary rule* is codified under Article 235, paragraph (5). Nevertheless, the new KUHAP does not yet regulate detailed authentication procedures, including standards for hash algorithms, digital chain-of-custody procedures, forensic imaging mechanisms, and certification systems for forensic experts. n contrast, the United States Federal Rules of Evidence have established an efficient self-authentication mechanism based on written certification by forensic experts, standardised hash-value procedures (particularly SHA-256), and properly documented chain-of-custody procedures. This comparison demonstrates that Indonesia already possesses a strong normative foundation but still requires a more comprehensive procedural framework. Second, the urgency of regulating the concept of self-authentication through hash values within Indonesian criminal procedure law lies in several important considerations: providing legal certainty for investigators, public prosecutors, judges, and defense counsel; improving judicial efficiency, particularly in light of the increasing number of cybercrime cases and other cases involving electronic evidence; ensuring international compatibility to support cross-jurisdictional cooperation; creating documented audit trails as a mechanism of law enforcement accountability; and protecting the rights of defendants through objectively verifiable standards. Based on these conclusions, this study recommends that the Government enact specific regulations governing the authentication of electronic evidence within criminal procedural law, as implementing regulations for Article 235 of the 2025 Criminal Procedure Code.

BIBLIOGRAPHY

Capra, Daniel. *Authenticating Digital Evidence*. Baylor Law Rev, 2017.

Committee, National Court Rules. Federal Rules of Evidence (2024). https://www.rulesofevidence.org/.

Dang, Quynh. "Recommendation for Applications Using Approved Hash Algorithms."

National, 2012. https://doi.org/https://doi.org/10.6028/NIST.SP.800-107r1.

Dewantoro. "AUTENTIKASI ALAT BUKTI ELEKTRONIK DALAM MEMPERLANCAR PEMBUKTIAN DI PERSIDANGAN PADA ERA DISRUPSI." *Jurnal Hukum Progresif* 12, no. 2 (2024): 135–51. https://doi.org/https://doi.org/10.14710/jhp.12.2.135-151.

Eoghan, Casey. *Digital Evidence and Computer Crime*. United States of America: Academic Press, 2011.

Ferner, Jens. "Digital Evidence in Germany: Legal Foundations, Collection, and Admissibility in Court." Ferner Alsdorf, 2025. https://www.ferner-alsdorf.com/digital-evidence-in-germany-legal-foundations-collection-and-admissibility-in-court/#:~:text=Post-mortem imaging (creating bit,the defense effectively raises doubt.

Fuady, Munir. *Teori Hukum Pembuktian Pidana Dan Perdata*. Cet. 2. Bandung: Citra Aditya Bakti, 2012.

Habiburrahman, Habiburrahman. "MD5 Di Era Post-Kriptografi : Studi Efektivitas Untuk Perlindungan Arsip Elektronik Pendahuluan." *Jurnal Ilmu Informasi Perpustakaan Dan Kearsipan* 14, no. 01 (2025): 9–18. https://doi.org/https://doi.org/10.24036/jiipk.v14i1.133546.

Haried, John M. "HOW TWO NEW RULES FOR SELF-AUTHENTICATION WILL SAVE YOU TIME AND MONEY." *Bolch Judicial Institute at Duke Law* 100, no. 4 (2021): 34–42.

Hon. Paul W. Grimm, Gregory P. Joseph, Daniel J. Capra. *Best Practices for Authenticating Digital Evidence.Pdf*. St.Paul,MN55101: West Academic Publishing, 2016.

Idris, Faizul, Hendratna Mutaqin, Magister Akuntansi, Fakultas Ekonomi, and Universitas Islam Bandung. "ANALISIS KEBERHASILAN DAN KEGAGALAN BUKTI FORENSIK DIGITAL DALAM SISTEM PERADILAN INDONESIA 'Study Kasus Putusan Nomor 130/Pid.Sus/2023/PN Ckr & Putusan Nomor 82/Pdt.G/2024/PA.Prob.'" *Journal of Golden Generation Legal Science* 2 (2026): 71–89. https://doi.org/https://doi.org/10.65244/jggls.v2i1.70.

Irianto, Yanto. "Judicial Adaptation to Digital Evidence in the Era of Cyber Governance." *Formosa Journal of Science and Technology (FJST)* 4, no. 9 (2025): 3015–30. https://doi.org/https://doi.org/10.55927/fjst.v4i9.248.

Isima, Nurlaila. "KEDUDUKAN ALAT BUKTI ELEKTRONIK DALAM PEMBUKTIAN PERKARA PIDANA." *Gorontalo Law Review* 5, no. 1 (2022): 179–89. https://doi.org/https://doi.org/10.32662/golrev.v5i1.1999.

Kent, Karent, and Dkk. "Guide to Integrating Forensic Techniques into Incident Response: Recommendations of the National Institute of Standards and Technology." National Institute of Standards and Technology (NIST), 2006. https://doi.org/https://doi.org/10.6028/NIST.SP.800-86.

Kiki Safitri, Dani Prabowo. "10 Tahun Pemerintahan Jokowi, Upaya Pemberantasan Kejahatan Siber Terus Meningkat." Kompas, 2024. https://nasional.kompas.com/read/2024/10/14/11503981/10-tahun-pemerintahan-jokowi-upaya-pemberantasan-kejahatan-siber-terus?page=all.

Kurnia, Erik A. "Eksepsi Resbob, Lokasi Perkara Dipersoalkan, Bukti Elektronik Diminta

Diuji Ulang." RadarSumedang.id, 2026. https://www.radarsumedang.id/bandung/2026/03/05/eksepsi-resbob-lokasi-perkara-dipersoalkan-bukti-elektronik-diminta-diuji-ulang/.

Maulitasari, Devi, and Rossi Passarella. *Teori Dan Sejarah Citra Forensik*. Pertama. Palembang: Unsri Press, 2020. https://repository.unsri.ac.id/92388/1/Teori dan Sejarah Citra Forensik.pdf.

Mualfah, Desti, and Rizdqi Akbar Ramadhan. "Analisis Forensik Metadata Kamera CCTV Sebagai Alat Bukti Digital." *Digital Zone: Jurnal Teknologi Informasi Dan Komunikasi* 11, no. 2 (2020): 257–67. https://doi.org/https://doi.org/10.31849/digitalzone.v11i2.5174.

Muladi & Barda Nawawi Arief. *Teori-Teori Dan Kebijakan Pidana*. 4th ed. Bandung: Alumni, 2010.

Nasrulloh, Imam Mahfudi, Sunardi Sunardi, and Imam Riadi. "ANALISIS FORENSIK SOLID STATE DRIVE (SSD) MENGGUNAKAN FRAMEWORK GRR RAPID RESPONSE FORENSIC ANALYSIS OF SOLID STATE DRIVES (SSD) USING THE GRR RAPID RESPONSE FRAMEWORK." *Jurnal Teknologi Informasi Dan Ilmu Komputer* 6, no. 5 (2019): 509–18. https://doi.org/10.25126/jtiik.201961516.

Rafli, Mutiaratu Astari. "Legality Of Authentic Deed With Cyber Notary Basis According To Legal Assurance Principles." *UNRAM LAW REVIEW* 6, no. 1 (2022). https://doi.org/https://doi.org/10.29303/ulrev.v6i1.225.

Sacvio Fath Senajaya, Handar Subhandi Bakhtiar, Slamet Tri Wahyudi. "Reformulasi Peraturan Digital Forensic Di Dalam Proses Pembuktian Perkara Tindak Pidana Korupsi Di Kejaksaan Agung Republik Indonesia." *Jurnal Kajian Hukum Dan Kebijakan Publik* 3, no. 2 (2026): 473–86. https://doi.org/https://doi.org/10.62379/av9bjg92.

Sekertariat Negara. "KUHP Dan KUHAP Baru Resmi Berlaku, Penegakan Hukum Di Indonesia Masuki Era Baru," 2026. https://www.setneg.go.id/baca/index/kuhp_dan_kuhap_baru_resmi_berlaku_penegakan_hukum_di_indonesia_masuki_era_baru.

Sinaga, Lasta Elfrida. "KUHAP 2025 Mengakui Bukti Elektronik: Bagaimana Autentikasinya?" Mangatur Nainggolan Law Firm, 2026. https://mnllaw.co.id/kuhap-2025-mengakui-bukti-elektronik-bagaimana-autentikasinya/.

Tunggati, Melki T. "Legal Validity of the Use of Graphonomy as an Evidentiary Instrument in Business Disputes in the Digital Age." *UNRAM LAW REVIEW* 9, no. 1 (2025). https://doi.org/https://doi.org/10.29303/ulrev.v9i1.404.

Undang-Undang Nomor 20 Tahun 2025 tentang Kitab Hukum Acara Pidana (2025).

Undang-Undang Nomor 8 Tahun 1981 tentang Hukum Acara Pidana (1981).

Vanessa, Vanessa, and Hery Firmansyah. "Analysis of the Validity of Electronic Evidence in Criminal Trial Proceedings and the Implementation of Its Admissibility (Judgment Study)." *Indonesian Jurnal Law and Economics Review* 20, no. 4 (2025). https://doi.org/https://doi.org/10.21070/ijler.v20i4.1395.